(12)特許協力条約に基づいて公開された国際出願 Publication

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月18 日 (18.08.2005)

PCT

(10) 国際公開番号
WO 2005/076519 A1

(51) 国際特許分類[7]: H04L 9/12, H03M 13/09, 13/19

(21) 国際出願番号: PCT/JP2004/001385

(22) 国際出願日: 2004 年2 月10 日 (10.02.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 松本 渉 (MATSUMOTO, Wataru) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 酒井 宏明 (SAKAI, Hiroaki); 〒1000013 東京都千代田区霞が関三丁目２番６号 東京倶楽部ビルディング 酒井国際特許事務所 Tokyo (JP).

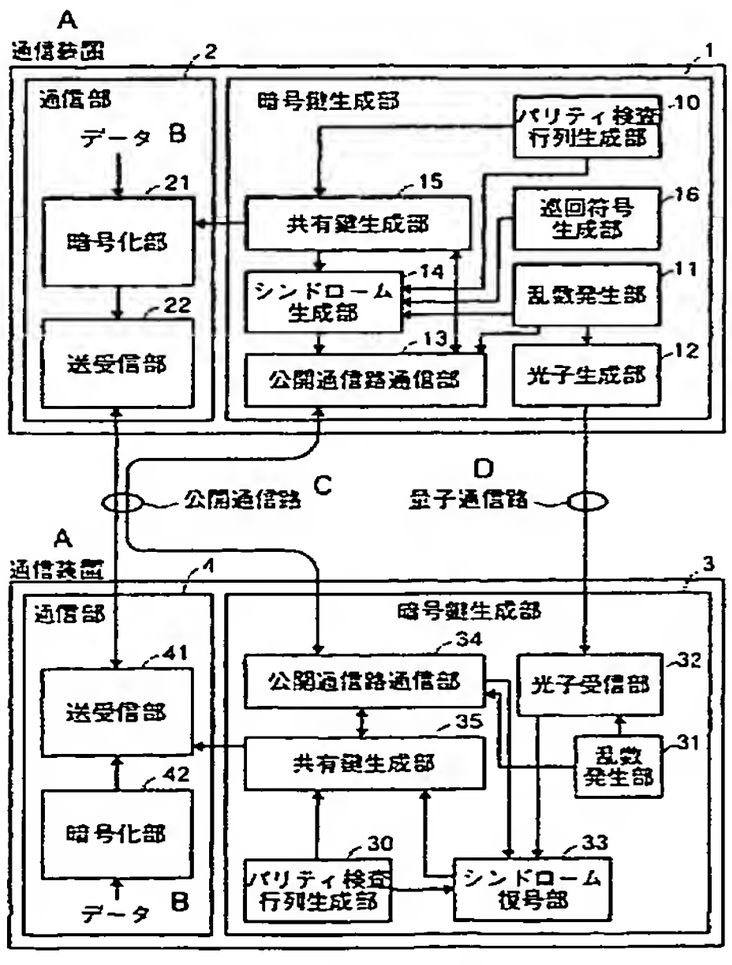
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH,

[続葉有]

(54) Title: QUANTUM KEY DELIVERING METHOD AND COMMUNICATION DEVICE

(54) 発明の名称: 量子鍵配送方法および通信装置



A...COMMUNICATION DEVICE
2...COMMUNICATION UNIT
B.. DATA
21...ENCRYPTING SECTION
22...TRANSMITTING/RECEIVING SECTION
1...ENCRYPTION KEY GENERATING UNIT
15...SHARED KEY GENERATING SECTION
14...SYNDROME GENERATING SECTION
13...OPEN COMMUNICATION PATH COMMUNICATION SECTION
10...PARITY CHECK MATRIX GENERATING SECTION
16...CYCLIC CODE GENERATING SECTION
11...RANDOM NUMBER GENERATING SECTION
12...PHOTON GENERATING SECTION
C...OPEN COMMUNICATION PATH
D...QUANTUM COMMUNICATION PATH
4...COMMUNICATION UNIT
41...TRANSMITTING/RECEIVING SECTION
42...ENCRYPTING SECTION
3...ENCRYPTION KEY GENERATING UNIT
34...OPEN COMMUNICATION PATH COMMUNICATION SECTION
35...SHARED KEY GENERATING SECTION
32...PHOTON RECEIVING SECTION
31...RANDOM NUMBER GENERATING SECTION
30...PARITY CHECK MATRIX GENERATING SECTION
33...SYNDROME DECRYPTING SECTION

(57) Abstract: A quantum key delivering method in which a communication device on the reception side corrects an error using a parity check matrix for LDPC code having an extremely high error correcting capability. The cyclic code syndrome generated by a communication device on the transmission side is compared with a deduced cyclic code syndrome generated according to a deduced word after error correction so as to detect an error in the deduced word.

(57) 要約: 本発明の量子鍵配送方法では、受信側の通信装置が、極めて高い誤り訂正能力をもつＬＤＰＣ符号用のパリティ検査行列を用いて誤り訂正を行うこととした。また、本発明の量子鍵配送方法では、送信側の通信装置が生成した巡回符号シンドロームと、誤り訂正後の推定語に基づいて生成した推定巡回符号シンドロームと、を比較し、前記推定語の誤り検出を行うこととした。

WO 2005/076519 A1

CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:
— 国際調査報告書